



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Notice of Breach

We are writing to tell you about a recent email incident that may have exposed some personal information maintained by NRI USA, LLC ("NRI") to unauthorized access. As a result of our investigation, we determined that some personal information that we maintained about a small number of our employees may have been accessed without authorization. We take this matter very seriously because we know how important your personal information is to you. At this time, we have no indication that any of this personal information has been inappropriately used by anyone. We are providing this notice to you as a precautionary measure, to inform you and to explain steps that you can take to help protect your information.

What happened:

On October 15, 2019, we learned that an unauthorized individual attempted to use one of our corporate email addresses to misdirect a payment intended for NRI. We immediately began an investigation and, based on the available evidence, determined that there had been unauthorized access to two (2) corporate email accounts between September 3, 2019 and October 23, 2019. Our investigation showed that the email accounts were used by employees from NRI and our related companies. On October 24, 2019, we determined that your personal information may have been accessed.

What information was involved:

The investigation revealed that in the process of obtaining information to misdirect the payment, the malicious actor may have accessed personal information in the email accounts. For this reason and because we could not identify what specific information was accessed, we reviewed the entire contents of each employee's email boxes to find out what was in each email, who may have been affected and where those people resided. That information may have included your <<b2b_text_1 (Impacted Data)>>.

What you can do:

Although we are unaware of any misuse of your or anyone's information, to help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring, at no cost to you, for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit <<IDMonitoringURL>> to activate and take advantage of your identity monitoring services.

You have until <<Date>> to activate your identity monitoring services.

Membership Number: <<Member ID>>

Additional information describing your services is included with this letter.

What we are doing:

When we discovered this incident, we immediately disabled the affected email accounts and had the users reset their passwords. To further enhance email and network security and to help prevent similar occurrences in the future, we have taken or will be taking the following steps:

1. Adding two-factor authentication for remote access to Office 365 services, including email;
2. Regular review of all remote logins to corporate email accounts;
3. Network-wide review of all forwarding rules;
4. Strengthening our filtering to help block dangerous emails;
5. Updating our response procedures to more quickly and effectively respond to incidents;
6. Adding a warning about phishing attempts and attempts to re-route payments to all emails; and
7. Enhancing our cyber training and providing regular communications in order to increase cyber awareness.

In addition, we are taking steps to mitigate any potential misuse of your information by offering you identity monitoring services and providing notice of this incident to appropriate regulators.

For important information:

Please know that the protection and security of your personal information is of our utmost priority, and we sincerely regret any concern or inconvenience that this matter may cause you. If you have any questions, please do not hesitate to call [1-888-888-8888](tel:1-888-888-8888), Monday through Friday, 6:00 a.m. to 3:30 p.m. Pacific Time.

Very truly yours,



Dean Stainton, CPHR
Director of People Experience

Additional Important Information

For residents of Hawaii, Michigan, Missouri, Virginia, Vermont, and North Carolina: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon, and West Virginia:

It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of Iowa:

State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon:

State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Maryland, Rhode Island, Illinois, New York, and North Carolina:

You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Maryland Office of the Attorney General Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202 1-888-743-0023 www.oag.state.md.us	Rhode Island Office of the Attorney General Consumer Protection 150 South Main Street Providence RI 02903 1-401-274-4400 www.riag.ri.gov	North Carolina Office of the Attorney General Consumer Protection Division 9001 Mail Service Center Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.com	Federal Trade Commission Consumer Response Center 600 Pennsylvania Ave, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft	New York Office of the Attorney General Bureau of Consumer Frauds & Protection The Capitol Albany, NY 12224-0341 1-800-771-7755 https://ag.ny.gov/consumer-frauds/identity-theft
--	---	---	---	---

For residents of Massachusetts: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf); TransUnion (<https://www.transunion.com/fraud-alerts>); or Experian (<https://www.experian.com/fraud:center.html>). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-

issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348
www.freeze.equifax.com
800-525-6285

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
www.experian.com/freeze
888-397-3742

TransUnion (FVAD)

P.O. Box 2000
Chester, PA 19022
freeze.transunion.com
800-680-7289

More information can also be obtained by contacting the Federal Trade Commission listed above.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you will have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.